Abstract

Given a set of elliptic curve points defined over a field F(p) and represented in projective coordinate, a method is presented which allows the embedding of data bits in both the X-coordinate and the Z-coordinate of the elliptic curve point when represented in projective coordinate. This makes the number of points that satisfy an elliptic curve equation and which can be used in the corresponding cryptosystem proportional to p^2 rather than p. This can be used to either increase security by making the bit positions where data bits are embedded known only to the sender and receiver. Alternatively, it can be used to increase the number of data bits that can be encrypted per single elliptic curve point encryption. In another alternative, it can also be used to reduce p. Also, it can be used as a countermeasure by randomizing the bit positions where data bits are embedded.
A similar formulation can be developed for elliptic curves over fields $F(2^m)$, as well as special elliptic curves such as Montgomery curves.